ABSTRACT OF THE DISCLOSURE

The invention concerns a method for protecting an electronic entity with encrypted access, against DFA (Differential Fault Analysis) attacks which consists in: storing the result of a selected step (R_m, K_n) of an iterative process forming part of the cryptographic algorithm and in performing once more at least part of the steps of said iterative process up to a new computation of a result corresponding to the one which has been stored, comparing the two results and denying distribution of an encrypted message (MC) if they are different.